CLAIMS

1. A method for negotiating the provision of a mobile IP service between a mobile node (MN) and a server (AAA server) in a network, the method including the steps of:

- providing an authentication protocol establishing a pass-through transport between said mobile node (MN) and said server (AAA server), and
- negotiating the provision of said mobile IP service via said authentication protocol over said pass-through transport.

2. The method of claim 1, characterized in that said authentication protocol is the Extensible Authentication Protocol (EAP).

3. The method of claim 2, characterized in that includes the step of selecting said transport as either of a level-2 or level-3 EAP transport.

4. The method of claim 2, characterized in that it includes the step of selecting said transport as IEEE 802.1x.

5. The method of claim 2, characterized in that it includes the step of selecting said transport as PANA.

6. The method of claim 2, characterized in that it includes the step of providing in said network a client node (AAA client) between said mobile node (MN) and said server (AAA server), wherein said client node (AAA client) plays a pass-through role and is not involved in said negotiation.

7. The method of claim 6, characterized in that it includes of providing between said client node (AAA client) and said server (AAA server) an EAP transport selected from the group consisting of Diameter and Radius.

8. The method of claim 6, characterized in that it includes the step of configuring said client node (AAA client) as a point of attachment to said network working as an Access Point.

9. The method of claim 6, characterized in that it includes the step of configuring said client node (AAA client) as a point of attachment to said network working as a router.

10. The method of claim 1 or 2, characterized in that said step of negotiating includes at least one of:

- authorizing said mobile node (MN) to use said mobile IP service,
- communicating to said mobile node (MN) a set of options for use of said mobile IP service,
- dynamically configuring a set of parameters required for using said mobile IP service, and
- configuring further options related to said mobile IP service.

11. The method of claim 2, characterized in that it includes the step of routing messages for activating said mobile IP service between said mobile node (MN) and said server (AAA server) via said Extensible Authentication Protocol (EAP) over said EAP transport upon at least one of said mobile node (MN) power up or connection of said mobile node (MN) to said network.

12. The method of claim 1 or 2, characterized in that it includes the step of

- providing in said network a home agent (HA) for communicating with said server (AAA server), and
- maintaining within said home agent (HA) configuration information for providing said mobile IP service.

13. The method of claim 12, characterized in that it includes the step of providing an AAA backbone protocol for transferring said configuration information between said home agent (HA) and said server (AAA server).

14. The method of claim 13, characterized in that said AAA backbone protocol is Diameter.

15. The method of claim 1 or 2, characterized in that it includes the step of performing, upon at least

one of said mobile node (MN) power up or connection of said mobile node (MN) to said network, a bootstrap procedure including steps selected from the group consisting of:

- authorizing said mobile node (MN) to use said mobile IP service,
- communicating to said mobile node (MN) options for use within said mobile IP service,
- configuring the parameters for use of said mobile IP service, and
- configuring service options communicated to said mobile node (MN).

16. The method of claim 15, characterized in that said parameters include at least one of: a home address for use by said nobile node (MN), the address of an associated home agent (HA) allotted thereto, cryptographic data for bootstrapping a security association (SA) with said Home Agent (HA).

17. The method of claim 1 or 2, characterized in that it includes the steps of:

- performing said method while said mobile node (MN) is roaming within a network different from the network of its Home Provider, and
- providing a proxy (AAA proxy) for communication between said mobile node (MN) and said server (AAA server) under said roaming conditions.

18. The method of claim 2, characterized in that it includes at least one of:

- said mobile node (MN) sending a respective identifier towards said server (AAA server),
- setting up a transport layer security (TLS) tunnel between said mobile node (MN) and said server (AAA) to protect authentication information,
- authenticating said mobile node (MN) with said server (AAA),

- closing said EAP communication after authenticating said mobile node (MN) and negotiating said mobile IP service therefore,

- negotiating a security association (SA) between said mobile node (MN) and a respective home agent (HA).

19. The method of claim 18, characterized in that it includes the step of said mobile node (MN) sending said identifier to said server (AAA server) as a Network Access Identifier (NAI).

20. The method of claim 18, characterized in that said step of setting up said TLS tunnel and authenticating said mobile node (MN) is conformant to the PEAPv2 protocol.

21. The method of claim 18, characterized in that it includes, in association with said authentication, the step of said mobile node (MN) and said server (AAA server) exchanging a set of attributes selected from attributes for authorising, negotiating and configuring said mobile IP network.

22. The method of claim 18, characterized in that said step of negotiating said security association (SA) involves an IKE negotiation.

23. The method of claim 18, characterized in that said authentication is based on a defined EAP method.

24. The method of claim 18, characterized in that said authentication is SIM-CARD based.

25. The method of claim 1 or 2, characterized in that said step of negotiating includes the step of said mobile node (MN) sending toward said server (AAA) a message including a set of information items selected from the group consisting of:

- service selection information items indicating the mobile node (MN) choice to activate said mobile IP service,

- service option information items, representative of the service options to be activated,

- an indication of a mobile node's preferred home agent (HA),

- an indication of a mobile node's preferred home address, and

- an interface identifier for use by a home agent (HA) for constructing the mobile node's home address.

26. The method of claim 1 or 2, characterized in that it includes the step of said mobile node (MN) sending negotiation messages with said server (AAA server) in the form of Type Length Value (TLV) messages.

27. The method of claim 1 or 2, characterized in that said step of negotiating includes said server (AAA) selectively identifying a home agent (HA) for providing said mobile IP service.

28. The method of claim 27, characterized in that it includes the step of:

- said server (AAA server) sending a home address request message to said home agent (HA) including an identifier (NAI) for said mobile node (MN),

- said home agent (HA) allotting a home address for said mobile node (MN).

29. The method of claim 28, characterized in that said step of allotting said home address involves either generating an interface identifier or utilizing a mobile node's indicated interface identifier.

30. The method of claim 28, characterized in that it includes the step of said home agent (HA) performing a duplicate address detection (DAD) for said home address.

31. The method of claim 30, characterized in that it includes, upon successful completion of said duplicate address detection (DAD), the step of said home agent (HA) preventing said home address allotted from being allocated to another user.

32. The method of claim 31, characterized in that it includes the steps of providing in said home agent

(HA) a binding cache and registering in said binding cache a dummy entry including said home address and an unspecified address as a care-of address, whereby any binding update (BU) reaching said home agent (HA) does not lead to the creation of a new entry.

33. The method of claim 1 or 2, characterized in that it includes the steps of:

- including in said network a home agent (HA) for providing said mobile IP service,

- configuring said server (AAA server) as a key distribution centre between said mobile node (MN) and said home agent (HA), and

- sending from said server (AAA server) to said mobile node (MN) and said home agent (HA) cryptographic information to permit bootstrapping a security association (SA) between said mobile node (MN) and said home agent (HA).

34. The method of claim 1 or 2, characterized in that it includes the steps of:

- including in said network a home agent (HA) for providing said mobile IP service, and

- said server (AAA server) sending to said home agent (HA) a Home Agent Configuration Request Message including information items selected from the group consisting of:

- an identifier for said mobile node (MN),

- an authorization lifetime indicating how long said mobile node (MN) is authorized to use said mobile IP service,

- bootstrap information for a security association (SA) between said mobile node (MN) and said home agent (HA), and

- a set of policies for said Home Agent (HA) to manage said mobile node's traffic.

35. The method of claim 34, characterized in that it includes the step of arranging said information

items in the form of Diameter Attribute Value Pairs (AVP).

36. The method of claim 34, characterized in that it includes the step of negotiating said security association (SA) via an IKE negotiation.

37. The method of claim 36, characterized in that said bootstrap information includes information items representative of at least one of:

- the authentication type to use for the first IKE phase,
- the key to use, and
- a respective lifetime for said key.

38. The method of claim 37, characterized in that it includes the step of setting said respective lifetime to an infinite value.

39. The method of claim 34, characterized in that it includes the step of providing in said network a home agent (HA) for communicating with said server (AAA server), and in that said set of policies includes information items representative of filtering rules to be enforced by said home agent (HA) on the mobile node (MN) traffic.

40. The method of claim 34, characterized in that it includes, in setting up said security association (SA) between said mobile node (MN) and said home agent (HA), at least one of:

- using a two phase IKE procedure using an aggressive mode in said first phase,
- using in said first IKE phase the care-of address in the place of the home address as the source address of the aggressive mode messages, and
- using the home address as the peer identifier for the mobile node (MN) in the second phase of said IKE procedure.

41. The method of claim 40, characterized in that it includes the step of said mobile node (MN) sending a binding update (BU) message to said home agent (HA) to

register its care-of address thereby activating said mobile IP service once said security association (SA) is negotiated.

42. The method of claim 2, characterized in that it includes the step of authenticating said mobile node (MN) with said server (AAA server) at least partly in parallel with said step of negotiating.

43. The method of claim 42, characterized in that it includes at least one of the steps of:

- said server (AAA server) sending an authorisation message for said mobile IP service within the EAP message starting said authentication step,
- upon receiving the indication from said mobile node (MN) to activate said mobile IP service, said server (AAA service) sending a home address request message toward a selected home agent (HA) while continuing said authentication of said mobile node (MN),
- said server (AAA server) continuing said authentication procedure of said mobile node (MN) by completing configuration of a respective home agent (HA) for providing said mobile IP service before completing said authentication procedure.

44. The method of claim 1 or 2, characterized in that it includes the step of causing said mobile node (MN) to perform a re-authentication step with said network in correspondence with at least one of:

- expiration of a given time-out interval, and
- said mobile node (MN) changing its point of attachment to said network.

45. The method of claim 44, characterized in that it includes the step of controlling the identity of said mobile node (MN) and its right to continue exploitation of said network at each said re-authentication.

46. The method of claim 44, characterized in that it includes the step of re-negotiating said mobile IP service upon each said re-authentication.

47. The method of claim 44, characterized in that it includes the steps of:

- checking whether said mobile IP service is active, and

- if said service is not active for said mobile node (MN), performing a new bootstrap phase by proposing activation of said mobile IP network to said Mobile node (MN).

48. The method of claim 44, characterized in that it includes the steps of:

- checking whether said mobile IP service is active,

- if said Mobile IP service is already active for said mobile node (MN) informing said mobile node (MN) of the status of said mobile IP service, and

- allowing said mobile node (MN) to select whether to maintain said mobile IP service unaltered, or permitting said mobile node (MN) to at least partly modify the configuration of said mobile IP service.

49. The method of claim 1 or 2, characterized in that it includes the steps of:

- setting up a mobile IP service session, and

- closing said session under the direction of said server (AAA server).

50. The method of claim 49, characterized in that said step of closing said session involves said server (AAA server) sending an Abort Session Request to at least one associated client node (AAA client, HA).

51. The method of claim 1 or 2, characterized in that it includes the steps of:

- setting up a mobile IP service session, and

- closing said session under the direction of said mobile node (MN).

52. The method of either of claims 49 or 51, characterized in that it includes the step of releasing the resources providing said mobile IP service upon closing said session.

53. The method of claim 2, characterized in that it includes the steps of:

- selecting said network as a network using a respective authentication method other than EAP,

- using said EAP transport for said step of negotiating, while providing authentication by said respective authentication method other than EAP.

54. The method of claim 53, characterized in that it includes the steps of:

- selecting said network as a cellular network including a GGSN node, and

- allotting to said mobile node (MN) an IP Address by activating a PDP context, whereby a direct communication channel is established between said mobile node (MN) and said GGSN node.

55. The method of claim 54, characterized in that it includes at least one of the steps of:

- said mobile node (MN) and said GGSN node setting up a PANA session,

- said GGSN node sending to said server (AAA server) an EAP request containing the user identifier (NAI) as well as an empty EAP packet, wherein said user identifier is inserted by said GGSN node,

- said server (AAA server) performing the negotiation phase of said services, and

- said server (AAA server) sending to said GGSN node an EAP SUCCESS message to be forwarded to said Mobile node (MN).

56. The method of claim 1 or 2, characterized in that it includes the step of said mobile node (MN) interrupting exploitation of said mobile IP service while maintaining connection to said network.

57. A system for negotiating the provision of a mobile IP service between a mobile node (MN) and a server (AAA server) in a network, the system including an authentication protocol for establishing a pass-through transport between said mobile node (MN) and said server (AAA server) and being configured for negotiating the provision of said mobile IP service via said authentication protocol over said pass-through transport.

58. The system of claim 57 characterized in that said authentication protocol is the Extensible Authentication Protocol (EAP)..

59. The system of claim 58, characterized in that said transport is either of a level-2 or level-3 EAP transport.

60. The system of claim 58, characterized in that said transport is IEEE 802.1x.

61. The system of claim 58, characterized in that said transport is PANA.

62. The system of claim 58, characterized in that it includes a client node (AAA client) between said mobile node (MN) and said server (AAA server), wherein said client node (AAA client) plays a pass-through role and is not involved in said negotiation.

63. The system of claim 62, characterized in that it includes, between said client node (AAA client) and said server (AAA server), an EAP transport selected from the group consisting of Diameter and Radius.

64. The system of claim 62, characterized in that said client node (AAA client) is a point of attachment to said network configured as an Access Point.

65. The system of claim 62, characterized in that said client node (AAA client) is a point of attachment to said network configured as a router.

66. The system of claim 57 or 58, characterized in that said system is configured for performing at least one of:

- authorizing said mobile node (MN) to use said mobile IP service,

- communicating to said mobile node (MN) a set of options for use of said mobile IP service,

- dynamically configuring a set of parameters required for using said mobile IP service, and

- configuring further options related to said mobile IP service.

67. The system of claim 58, characterized in that said system is configured for routing messages for activating said mobile IP service between said mobile node (MN) and said server (AAA server) via said Extensible Authentication Protocol (EAP) over said EAP transport upon at least one of said mobile node (MN) power up or connection of said mobile node (MN) to said network.

68. The system of claim 57 or 58, characterized in that it includes a home agent (HA) for communicating with said server (AAA server), and maintaining configuration information for providing said mobile IP service.

69. The system of claim 68, characterized in that it includes an AAA backbone protocol for transferring said configuration information between said home agent (HA) and said server (AAA server).

70. The system of claim 69, characterized in that said AAA backbone protocol is Diameter.

71. The system of claim 57 or 58, characterized in that said system is configured for performing, upon at least one of said mobile node (MN) power up or connection of said mobile node (MN) to said network, a bootstrap procedure including steps selected from the group consisting of:

- authorizing said mobile node (MN) to use said mobile IP service,

- communicating to said mobile node (MN) options for use within said mobile IP service,

- configuring the parameters for use of said mobile IP service, and

- configuring service options communicated to said mobile node (MN).

72. The system of claim 71, characterized in that said parameters include at least one of: a home address for use by said mobile node (MN), the address of an associated home agent (HA) allotted thereto, cryptographic data for bootstrapping a security association (SA) with said Home Agent (HA).

73. The system of claim 57 or 58, characterized in that it includes a proxy (AAA proxy) for communication between said mobile node (MN) and said server (AAA server) while said mobile node (MN) is roaming with a network different from the network of its Home Provider.

74. The system of claim 58, characterized in that it includes at least one of:

- an EAP communication transport between said mobile node (MN) and said server (AAA server), whereby said mobile node (MN) is able to send a respective identifier towards said server (AAA server),

- a transport layer security (TLS) tunnel between said mobile node (MN) and said server (AAA) to protect authentication information,

- an authentication function for authenticating said mobile node (MN) with said server (AAA),

- an EAP communication closing function for closing said EAP communication after authenticating said mobile node (MN) and negotiating said mobile IP service therefor,

- a security association (SA) between said mobile node (MN) and a respective home agent (HA).

75. The system of claim 74, characterized in that said mobile node (MN) is configured for sending said identifier to said server (AAA server) as a Network Access Identifier (NAI).

76. The system of claim 74, characterized in that at least one of said TLS tunnel and said authentication function is conformant to the PEAPv2 protocol.

77. The system of claim 74, characterized in that it includes, in association with said authentication, a set of attributes to be exchanged between said mobile node (MN) and said server (AAA server), said set of attributes selected from attributes for authorising, negotiating and configuring said mobile IP network.

78. The system of claim 74, characterized in that said security association (SA) is based on an IKE negotiation.

79. The system of claim 74, characterized in that said authentication is based on a defined EAP system.

80. The system of claim 74, characterized in that said authentication is SIM-CARD based.

81. The system of claim 57 or 58, characterized in that said mobile node (MN) is configured for sending toward said server (AAA) a message including a set of information items selected from the group consisting of:

- service selection information items indicating the mobile node (MN) choice to activate said mobile IP service,
- service option information items, representative of the service options to be activated,
- an indication of a mobile node's preferred home agent (HA),
- an indication of a mobile node's preferred home address, and
- an interface identifier for use by a home agent (HA) for constructing the mobile node's home address.

82. The system of claim 57 or 58, characterized in that said mobile node (MN) is configured for sending negotiation messages with said server (AAA server) in the form of Type Length Value (TLV) messages.

83. The system of claim 57 or 58, characterized in that said server (AAA) is configured for selectively identifying a home agent (HA) for providing said mobile IP service.

84. The system of claim 83, characterized in that

- said server (AAA server) is configured for sending a home address request message to said home agent (HA) including an identifier (NAI) for said mobile node (MN),

- said home agent (HA) is configured for allotting a home address to said mobile node (MN).

85. The system of claim 84, characterized in that said home agent (HA) is configured for allotting said home address either by generating an interface identifier or by utilizing a mobile node's indicated interface identifier.

86. The system of claim 84, characterized in that said home agent (HA) is configured for performing a duplicate address detection (DAD) for said home address.

87. The system of claim 86, characterized in that said home agent (HA) is configured for preventing said home address allotted from being allocated to another user upon successful completion of said duplicate address detection (DAD).

88. The system of claim 87, characterized in that said home agent (HA) has a binding cache and is configured for registering in said binding cache a dummy entry including said home address and an unspecified address as a care-of address whereby any binding update (BU) reaching said home agent (HA) does not lead to the creation of a new entry.

89. The system of claim 57 or 58, characterized in that it includes:

- a home agent (HA) for providing said mobile IP service,

- said server (AAA server) configured as a key distribution centre between said mobile node (MN) and said home agent (HA), for sending to said mobile node (MN) and said home agent (HA) cryptographic information to permit bootstrapping a security association (SA) between said mobile node (MN) and said home agent (HA).

90. The system of claim 57 or 58, characterized in that it includes:

- a home agent (HA) for providing said mobile IP service, and

- said server (AAA server) configured for sending to said home agent (HA) a Home Agent Configuration Request Message including information items selected from the group consisting of:

- an identifier for said mobile node (MN),

- an authorisation lifetime indicating how long said mobile node (MN) is authorized to use said mobile IP service,

- bootstrap information for a security association (SA) between said mobile node (MN) and said home agent (HA), and

- a set of policies for said Home Agent (HA) to manage said mobile node's traffic.

91. The system of claim 90, characterized in that said information items are in the form of Diameter Attribute Value Pairs (AVP).

92. The system of claim 90, characterized in that said security association (SA) is an IKE negotiated security association.

93. The system of claim 92, characterized in that said bootstrap information includes information items representative of at least one of:

- the authentication type to use for the first IKE phase,

- the key to use, and

- a respective lifetime for said key.

94. The system of claim 93, characterized in that said respective lifetime is set to an infinite value.

95. The system of claim 90, characterized in that said network includes a home agent (HA) for communicating with said server (AAA server) and in that said set of policies includes information items representative of filtering rules to be enforced by said home agent (HA) on the mobile node (MN) traffic.

96. The system of claim 90, characterized in that said security association (SA) is based on at least one of:

- a two phase IKE procedure using an aggressive mode in said first phase,
- the care-of address being used in the place of the home address as the source address of the aggressive mode messages in said first IKE phase, and
- the home address being used as the peer identifier for the mobile node (MN) in the second phase of said IKE procedure.

97. The system of claim 96, characterized in that said mobile node (MN) is configured for sending a binding update (BU) message to said home agent (HA) to register its care-of address thereby activating said mobile IP service once said security association (SA) is negotiated.

98. The system of claim 58, characterized in that the system is configured for authenticating said mobile node (MN) with said server (AAA server) at least partly in parallel with said step of negotiating.

99. The system of claim 98, characterized in that the system is configured for performing at least one of the steps of:

- said server (AAA server) sending an authorisation message for said mobile IP service within the EAP message starting said authentication step,
- upon receiving the indication from said mobile node (MN) to activate said mobile IP service, said

server (AAA service) sending a home address request message toward a selected home agent (HA) while continuing said authentication of said mobile node (MN),

- said server (AAA server) continuing said authentication procedure of said mobile node (MN) by completing configuration of a respective home agent (HA) for providing said mobile IP service before completing said authentication procedure.

100. The system of claim 57 or 58, characterized in that said mobile node (MN) is configured for performing a re-authentication step with said network in correspondence with at least one of:

- expiration of a given time-out interval, and
- said mobile node (MN) changing its point of attachment to said network.

101. The system of claim 100, characterized in that the system is configured for controlling the identity of said mobile node (MN) and its right to continue exploitation of said network at each said re-authentication.

102. The system of claim 100, characterized in that the system is configured for re-negotiating said mobile IP service upon each said re-authentication.

103. The system of claim 100, characterized in that the system is configured for:

- checking whether said mobile IP service is active, and
- if said service is not active for said mobile node (MN), performing a new bootstrap phase by proposing activation of said mobile IP network to said Mobile node (MN).

104. The system of claim 100, characterized in that the system is configured for:

- checking whether said mobile IP service is active,

- if said Mobile IP service is already active for said mobile node (MN) informing said mobile node (MN) of the status of said mobile IP service, and

- allowing said mobile node (MN) to select whether to maintain said mobile IP service unaltered, or permitting said mobile node (MN) to at least partly modify the configuration of said mobile IP service.

105. The system of claim 57 or 58, characterized in that the system is configured for:

- setting up a mobile IP service session, and

- closing said session under the direction of said server (AAA server).

106. The system of claim 105, characterized in that the system is configured for said step of closing said session involving said server (AAA server) sending an Abort Session Request to at least one associated client node (AAA client, HA).

107. The system of claim 57 or 58, characterized in that the system is configured for:

- setting up a mobile IP service session, and

- closing said session under the direction of said mobile node (MN).

108. The system of either of claims 105 or 107, characterized in that the system is configured for releasing the resources providing said mobile IP service upon closing said session.

109. The system of claim 58, characterized in that said network is a network having a respective authentication function other than EAP and said system is configured for using said EAP transport for said step of negotiating, while providing authentication by said respective authentication function other than EAP.

110. The system of claim 109, characterized in that said network is a cellular network including a GGSN node, and the system is configured for allotting to said mobile node (MN) an IP Address by activating a PDP context, whereby a direct communication channel is

established between said mobile node (MN) and said GGSN node.

111. The system of claim 110, characterized in that:

- said mobile node (MN) and said GGSN node are configured for setting up a PANA session,

- said GGSN node is configured for sending to said server (AAA server) an EAP request containing the user identifier (NAI) as well as an empty EAP packet, wherein said user identifier is inserted by said GGSN node,

- said server (AAA server) is configured for performing the negotiation phase of said services, and

- said server (AAA server) is configured for sending to said GGSN node an EAP SUCCESS message to be forwarded to said Mobile node (MN).

112. The system of claim 57 or 58, characterized in that said mobile node (MN) is configured for interrupting exploitation of said mobile IP service while maintaining connection to said network.

113. A network including a server (AAA server) and at least one mobile node (MN) having associated a system according to any one of claims 57 to 112.

114. A terminal adapted for negotiating with a server (AAA server) the provision of a mobile IP service in a network, the network including an authentication protocol for establishing a pass-through transport between said terminal (MN) and said server (AAA server), wherein said terminal comprises at least one module for automatically collecting from the server (AAA server) and via said pass-through transport initialisation parameters for negotiating the provision of the Mobile IP service.

115. The terminal of claim 114 comprising a memory device for storing said module.

116. A server (AAA server) adapted for negotiating with a mobile node (MN) the provision of a mobile IP

service in a network, the network including an authentication protocol for establishing a pass-through transport between said server (AAA server) and said mobile node (MN), wherein said server (AAA server) comprises at least one module to control in a centralized way the initialisation of the Mobile IP service by providing configuration information to the mobile node (MN) via said pass-through transport.

117. The server of claim 116 comprising a memory device for storing said module.

118. A computer program product loadable in the memory of at least one computer and including software code portions for performing the steps of any of claims 1 to 56.